UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/930,029	08/14/2001	William B. Sweet	055120-0002	3170

7590 04/05/2006

William Sweet
2665 North First St
Suite 300
San Jose, CA 95134

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 04/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/930,029	SWEET ET AL.	
	Examiner	Art Unit	
	Jeffrey D. Popham	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22 and 52-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22 and 52-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Remarks

Claims 1-22 and 52-58 are pending.

Response to Arguments

Applicant's arguments, see Remarks, filed 1/13/2006, with respect to the rejection(s) of claim(s) 1-22 and 52-58 under 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made with Win (U.S. Patent 6,161,139) in view of Berson (U.S. Patent 6,754,821), Woodward (Woodward, John, "Comments on Private Sector Use of Biometrics and the Need for Limited Government Action", 7/17/1998, pp. 1-12, obtained from http://www.ntia.doc.gov/ntiahome/privacy/mail/disk/Woodward.htm), and Shintani (U.S. Patent 6,137,480).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claims 1, 15, 16, 18-22, 52, and 54-57 are rejected under 35 U.S.C. 102(e) as being anticipated by Win (U.S. Patent 6,161,139).

Regarding Claim 1,

Win discloses a method for providing cryptographic capabilities to a plurality of network users over a decentralized public network, comprising:

Receiving a request for an access permission security profile on behalf of a network user (Column 9, lines 25-45);

Authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40);

Creating the access permission security profile, to be used in forming a cryptographic key for enabling the network user to decrypt selected portions of an encrypted object and to encrypt selected portions of a plaintext object (Column 10, lines 26-40); and

Securely transmitting the access permission security profile to the network user over the network (Column 10, lines 41-49).

Regarding Claim 15,

Win discloses the method of claim 1, in addition, Win discloses that the request is initiated in-band by the network user over the network (Column 9, lines 25-35).

Regarding Claim 16,

Win discloses the method of claim 1, in addition, Win discloses that the access permission security profile is in the form of a token that is adaptable to expire (Column 10, lines 50-62).

Regarding Claim 18,

Win discloses the method of claim 1, in addition, Win discloses that the authenticating step includes the use of a hardware token (Column 27, lines 28-40).

Regarding Claim 19,

Win discloses the method of claim 1, in addition, Win discloses that the authenticating step includes the use of a software token (Column 17, lines 24-33).

Regarding Claim 20,

Win discloses the method of claim 1, in addition, Win discloses that the authenticating step includes the use of a user password (Column 9, lines 25-35).

Regarding Claim 21,

Win discloses the method of claim 1, in addition, Win discloses that the authenticating step includes the use of a record of time at which the request was made (Column 9, lines 46-52).

Regarding Claim 22,

Win discloses the method of claim 1, in addition, Win discloses that the authenticating step includes the use of a record of the user's physical location (Column 15, lines 46-60).

Regarding Claim 52,

Win discloses a centralized security management system for distributing cryptographic capabilities to a plurality of network users over a decentralized public network, comprising:

A plurality of member tokens for providing cryptographic capabilities to authenticated users of the decentralized public network (Column 13, lines 32-44);

A set if server systems for managing the distribution of member tokens (Figure 1);

Means for requesting a member token from at least one server system (Column 9, lines 25-45);

A set of client systems (Column 4, lines 10-44), wherein each client system includes means for receiving the requested member token (Column 10, lines 26-49) and means for utilizing the cryptographic capabilities provided by the member token (Column 7, line 53 to Column 8, line 16); and

Means for securely distributing a requested member token from at least one server system to at least one client system over the decentralized public network (Column 10, lines 41-49).

Regarding Claim 54,

Win discloses that the means for requesting a member token resides on each client system (Column 9, lines 25-45).

Regarding Claim 55,

Win discloses that means for authenticating a user resides on at least one server system (Column 10, lines 26-40).

Regarding Claim 56,

Win discloses that managing the distribution of member tokens includes dynamic updating of the member tokens (Column 17, lines 37-48).

Regarding Claim 57,

Win discloses the method of claim 1 and the system of claim 52, in addition, Win discloses that the decentralized public network is the Internet (Column 4, lines 46-57).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 2-16, 18-22, 57, and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of Berson (U.S. Patent 6,754,821).

Regarding Claim 2,

Win discloses that the creating step comprises:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities (Column 10, lines 26-49; and Column 13, lines 32-44); and

Creating one or more security profiles for each network user (Column 13, lines 32-44);

But does not disclose establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key, or that the security profiles contain at least one of these access codes.

Berson, however, discloses establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key (Column 3, lines 23-34; and Column 5, lines 20-35); and

That each network user's security profile contains at least one access code (Column 5, line 20 to Column 6, line 8).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the transition state-based cryptography system of Berson into the role-based access control system of Win in order to allow an entire file, program, etc. to be downloaded/acquired at first, while controlling access to

different/progressive sections of the data based upon predetermined conditions that the user must meet prior to decryption of the additional sections.

Regarding Claim 3,

Win as modified by Berson discloses the method of claim 2, in addition, Win discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup, or domain (Column 13, lines 32-44).

Regarding Claim 4,

Win discloses a method for providing decryption capabilities to a plurality of network users over a decentralized public network, comprising:

Receiving a request for decryption capabilities on behalf of a network user (Column 9, lines 25-45);

Authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40);

Creating an access permission security profile to be used in forming a cryptographic key for enabling the network user to decrypt an encrypted object (Column 10, lines 26-40);

Receiving from the user information associated with the encrypted object (Column 7, line 53 to Column 8, line 3); and

Session/transaction encryption (Column 22, lines 15-65);

But does not disclose generating a cryptographic key using the access permission security profile and the received information associated with the encrypted object, and securely transmitting the cryptographic key to the network user over the network.

Berson, however, discloses generating a cryptographic key using the access permission security profile and the received information associated with the encrypted object (Column 5, line 56 to Column 6, line 8); and securely transmitting the cryptographic key to the network user over the network (Column 5, line 36 to Column 6, line 8). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the transition state-based cryptography system of Berson into the role-based access control system of Win in order to allow an entire file, program, etc. to be downloaded/acquired at first, while controlling access to different/progressive sections of the data based upon predetermined conditions that the user must meet prior to decryption of the additional sections.

Regarding Claim 5,

Win as modified by Berson discloses the method of claim 4, in addition, Win discloses that the creating step comprises:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities (Column 10, lines 26-49; and Column 13, lines 32-44); and

Creating one or more security profiles for each network user (Column 13, lines 32-44); and

Berson discloses establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key (Column 3, lines 23-34; and Column 5, lines 20-35); and

That each network user's security profile contains at least one access code (Column 5, line 20 to Column 6, line 8).

Regarding Claim 6,

Win as modified by Berson discloses the method of claim 5, in addition, Win discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain (Column 13, lines 32-44).

Regarding Claim 7,

Win discloses a method for cryptographically securing the distribution of information over a decentralized public network to a plurality of network users, comprising:

Creating a computer representable data object (Column 14, line 25 to Column 15, line 14);

Creating one or more access permission credentials (Column 17, line 65 to Column 18, line 10);

Assigning an access permission credential to each of the data objects, wherein the access permission credential ensures that only authorized users are able to access the data objects (Column 17, line 65 to Column 18, line 57);

Authorizing at least one network user from the plurality of network users (Column 8, lines 17-44); and

Transmitting the data object over the network (Column 8, lines 45-60);

But does not disclose the encryption of embedded objects within each data object, or the access to/decryption of selected embedded objects.

Berson, however, discloses that a data object includes one or more embedded objects (Column 3, lines 23-34; and Column 5, lines 20-35);

Selecting one or more embedded objects of the data object to be encrypted (Column 3, lines 23-34; and Column 5, lines 20-35);

Encrypting the selected embedded objects (Column 3, lines 23-34; and Column 5, lines 20-35); and

Assigning an access permission credential to each of the selected embedded objects, wherein the access permission credential ensures that only authorized users are able to decrypt encrypted embedded objects of the data object (Column 5, line 20 to Column 6, line 8).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the transition state-based cryptography system of Berson into the role-based access control system of Win in order to allow an entire file, program, etc. to be downloaded/acquired at first, while controlling access to different/progressive sections of the data based upon predetermined conditions that the user must meet prior to decryption of the additional sections.

Regarding Claim 8,

Win as modified by Berson discloses the method of claim 7, in addition, Win discloses that the information is digital content (Column 9, lines 26-35).

Regarding Claim 9,

Win as modified by Berson discloses the method of claim 7, in addition, Win discloses that the authorizing step includes:

Receiving a request for an access permission security profile on behalf of a network user (Column 9, lines 25-45);

Authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40); and

Securely transmitting the security profile to the network user over the network (Column 10, lines 41-49).

Regarding Claim 10,

Win as modified by Berson discloses the method of claim 7, in addition, Win discloses that the authorizing step includes:

Sending a request for an access permission security profile on behalf of a network user to a centralized server system over the network (Column 9, lines 25-45);

Receiving the request at the central server system (Column 9, lines 25-45);

Authenticating the request (Column 9, lines 36-45; and Column 10, lines 26-40); and

Securely transmitting the access permission security profile from the server system to the network user over the network (Column 10, lines 41-49).

Regarding Claim 11,

Win as modified by Berson discloses the method of claim 7, in addition, Win discloses that the authorizing step is automatic and based upon the user's possession of an access permission security profile (Column 10, lines 26-40).

Regarding Claim 12,

Win as modified by Berson discloses the method of claim 7, in addition, Berson discloses that the encrypting step comprises:

Identifying a group of network users who are to be allowed access to a data object to be encrypted (Column 5, lines 20-35);

Generating an appropriate cryptographic credential key from a set of credential categories, the credential key relating to the group of network users (Column 5, lines 20-35);

Generating a cryptographic working key from at least a domain component (information for the state), a maintenance component (information regarding progression), and a pseudorandom component (Column 5, lines 20-35; Column 5, line 56 to Column 6, line 8; and Column 6, lines 55-65);

Encrypting the pseudorandom component with the credential key (Column 5, line 56 to Column 6, line 8; and Column 6, lines 55-65); and

Associating the encrypted pseudorandom component to the encrypted data object (Column 5, line 56 to Column 6, line 8; and Column 6, lines 55-65).

In this embodiment, the pseudorandom data is encrypted under the progressive credential keys, with a portion of the pseudorandom data being encrypted under each key.

Regarding Claim 13,

Win as modified by Berson discloses the method of claim 10, in addition, Win discloses that the access permission security profile is created by:

Identifying one or more groups of network users who are to be provided with cryptographic capabilities (Column 10, lines 26-49; and Column 13, lines 32-44); and

Creating one or more security profiles for each network user (Column 13, lines 32-44);

But does not disclose establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key, or that the security profiles contain at least one of these access codes.

Berson, however, discloses establishing one or more access codes for each group, wherein each access code is adapted to be combined with other components to form a cryptographic key (Column 3, lines 23-34; and Column 5, lines 20-35); and

That each network user's security profile contains at least one access code (Column 5, line 20 to Column 6, line 8).

Regarding Claim 14,

Win discloses that each group is a category, organization, organization unit, role, work project, geographical location, workgroup or domain (Column 13, lines 32-44).

Regarding Claim 15,

Win as modified by Berson discloses the methods of claims 4 and 9, in addition, Win discloses that the request is initiated in-band by the network user over the network (Column 9, lines 25-35).

Regarding Claim 16,

Win as modified by Berson discloses the methods of claims 4, 9, 10, and 11, in addition, Win discloses that the access permission security profile is in the form of a token that is adaptable to expire (Column 10, lines 50-62).

Regarding Claim 18,

Win as modified by Berson discloses the methods of claims 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a hardware token (Column 27, lines 28-40).

Regarding Claim 19,

Win as modified by Berson discloses the methods of claims 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a software token (Column 17, lines 24-33).

Regarding Claim 20,

Win as modified by Berson discloses the methods of claims 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a user password (Column 9, lines 25-35).

Regarding Claim 21,

Win as modified by Berson discloses the methods of claims 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a record of time at which the request was made (Column 9, lines 46-52).

Regarding Claim 22,

Win as modified by Berson discloses the methods of claims 4, 9, and 10, in addition, Win discloses that the authenticating step includes the use of a record of the user's physical location (Column 15, lines 46-60).

Regarding Claim 57,

Win as modified by Berson discloses the methods of claims 4 and 7, in addition, Win discloses that the decentralized public network is the Internet (Column 4, lines 46-57).

Regarding Claim 58,

Win discloses the method of claim 1 and the system of claim 52. Win as modified by Berson discloses the methods of claims 4 and 7.

Win discloses that the decentralized public network is a cellular phone network (Column 26, lines 32-47). Berson also discloses that the decentralized public network is a cellular phone network (Column 2, lines 9-21).

Regarding Claims 1 and 52, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the transition state-based cryptography system of Berson into the role-

based access control system of Win in order to allow an entire file, program, etc. to be downloaded/acquired at first, while controlling access to different/progressive sections of the data based upon predetermined conditions that the user must meet prior to decryption of the additional sections.

3. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of Woodward (Woodward, John, "Comments on Private Sector Use of Biometrics and the Need for Limited Government Action", 7/17/1998, pp. 1-12, obtained from http://www.ntia.doc.gov/ntiahome/privacy/mail/disk/Woodward.htm).

Win does not disclose that the authenticating step includes the use of biometric information.

Woodward, however, discloses that the authenticating step includes the use of biometric information (Pages 5-7, Section III). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the biometric searching techniques of Woodward into the role-based access control system of Win in order to provide a way to authenticate a user that is not based on a credential (such as a password) that can be easily compromised, thus enhancing reliability of the system's authentication.

4. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of Berson, further in view of Woodward.

Win as modified by Berson does not disclose that the authenticating step includes the use of biometric information.

Woodward, however, discloses that the authenticating step includes the use of biometric information (Pages 5-7, Section III). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the biometric searching techniques of Woodward into the role-based access control system of Win as modified by Berson in order to provide a way to authenticate a user that is not based on a credential (such as a password) that can be easily compromised, thus enhancing reliability of the system's authentication.

5. Claim 53 is rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of Shintani (U.S. Patent 6,137,480).

Win does not disclose that each client system further includes user authentication means.

Shintani, however, discloses that each client system further includes user authentication means (Column 2, line 61 to Column 3, line 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication card system of Shintani into the role-based access control system of Win in order to enhance service to a user and security of data on a computer by only allowing a user to use the computer when he is

authenticated and in close proximity to the computer, and by disabling access to the computer when the user leaves the computer.

6. Claim 53 is rejected under 35 U.S.C. 103(a) as being unpatentable over Win in view of Berson, further in view of Shintani.

Win as modified by Berson does not disclose that each client system further includes user authentication means.

Shintani, however, discloses that each client system further includes user authentication means (Column 2, line 61 to Column 3, line 3). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the authentication card system of Shintani into the role-based access control system of Win as modified by Berson in order to enhance service to a user and security of data on a computer by only allowing a user to use the computer when he is authenticated and in close proximity to the computer, and by disabling access to the computer when the user leaves the computer.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffrey D Popham
Examiner
Art Unit 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER

Notice of References Cited	Application/Control No. 09/930,029	Applicant(s)/Patent Under Reexamination SWEET ET AL.	
	Examiner Jeffrey D. Popham	Art Unit 2137	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,161,139 A	12-2000	Win et al.	709/225
*	B	US-6,754,8[illegible]1 B1	06-2004	Berson et al.	713/170
*	C	US-6,137,480 A	10-2000	Shintani, Peter	345/169
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Woodward, John, "Comments on Private Sector Use of Biometrics and the Need for Limited Government Action", 7/17/1998, pp. 1-12, obtained from http://www.ntia.doc.gov/ntiahome/privacy/mail/disk/Woodward.htm
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Comments Focusing on Private Sector Use of Biometrics and the Need for Limited Government Action

by

John D. Woodward, Jr.

Attorney-at-Law

For the National Telecommunications and Information Administration,

U.S. Department of Commerce

On "Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy"

July 17, 1998 Washington, D.C.

I. Introduction

From activities as diverse as the elaborate security of the Winter Olympics in Nagano, Japan to the daily operations of the Purdue Employees Federal Credit Union in the Hoosier State, both the public and private sectors are making extensive use of biometrics. This new technological reality relies on "the body as password" for human recognition purposes to provide better security, increased efficiency and improved service.

In technical terms, biometrics is the automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic or trait to a database for purposes of recognizing that individual. As this technology becomes more economically viable, technically perfected and widely deployed, biometrics will become the passwords and personal identification numbers (PINs) of the twenty-first century. In the process, biometrics could refocus the way Americans look at the brave new world of personal information.

In discussing biometrics, these comments address a central question: Are new protections for privacy necessary or even desirable in the face of the new technological reality of biometrics? In a prospective way, I hope to identify relevant legal and policy concerns related to the private sector's use of

biometrics. I then discuss a workable "biometric blueprint" based on limited government regulation that will hopefully provide a helpful framework for further work and deliberations.(1)

Information privacy concerns related to private sector use of biometrics, which would include Internet applications, can be effectively accommodated by a federally-mandated biometric blueprint based on a Code of Fair Information Practices (CFIP). In essence, such a biometric blueprint would require that an individual have notice of and give consent to the use of his biometric identification information. Moreover, organizations using biometric identification information would be required by law to safeguard their databases and to permit the individual to correct any mistakes in the data collected.

As the executive and legislative branches get more involved with biometrics, three important points need to be stressed at the outset:

1. Biometrics should not be construed as privacy's foe. Quite to the contrary, biometrics is privacy's friend. Biometrics is privacy's friend because biometrics:

Safeguards information integrity and thwarts identity theft;

Limits access to sensitive information; and,

Serves as a privacy enhancing technology.

2. A pro-privacy position should not be construed as an anti-biometric stance: You can be a friend of privacy and a friend of biometrics. Moreover, limited government regulation of private sector use of this technology is not opposing biometrics but rather promoting biometrics. Appropriate policymaking can greatly increase public acceptance of this technology.

3. The law and policy concerns of biometrics cannot be left solely to politicians, lawyers and advocates. Technologists, engineers and scientists must vigorously add their voices to this discussion because we need the benefit of their unique scientific and technical understanding.

II. How Are Privacy Concerns Implicated by Biometrics Safeguarded Under the Status Quo?

A. Examination of the Legal Status Quo

Since privacy concerns are central to biometrics, we first have to define privacy in a legal context. The word "privacy" (like the word "biometrics") is nowhere to be found in the text of the United States Constitution. Perhaps the absence of a textual reference to privacy makes the legal community all the more fond of defining what privacy is and explaining what it should be. Privacy is different things to different people. Most importantly for the context of biometrics, privacy includes a control aspect -- "control we have over information about ourselves", "[c]ontrol over who can sense us", "...control over the intimacies of personal identity" or as a federal appeals court has phrased it, "control over knowledge about oneself. But it is not simply control over the quantity of information abroad; there are modulations in the quality of knowledge as well."(2)

Thus information privacy, or control over information about ourselves, lies at the very heart of the privacy concerns raised by this new technology because individuals have an interest in determining how, when, why and to whom information about themselves, in the form of biometric identification information, would be disclosed.

In the American legal experience, privacy protections have followed two basic pathways depending on whether the source of the privacy intrusion is a governmental or private sector activity. While privacy is not explicitly cited in the text, the Constitution, through the Bill of Rights, protects the individual from government's intrusion into the individual's privacy. For example, the Bill of Rights contains privacy protections in the First Amendment rights of freedom of speech, press and association; the Third Amendment prohibition against the quartering of soldier's in one's home; the Fourth Amendment right to be free from unreasonable searches and seizures; the Fifth Amendment right against self-incrimination; and the Ninth Amendment's provision that "[t]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people;" and the Tenth Amendment's provision that "[t]he powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."

With respect to private sector actions, the Constitution traditionally embodies what is essentially a *laissez-faire* spirit. As constitutional law scholar Laurence Tribe has noted, "[T]he Constitution, with the sole exception of the Thirteenth Amendment prohibiting slavery, regulates action by the government rather than the conduct of private individuals and groups." With respect to the conduct of private individuals, the Supreme Court has been reluctant to find a privacy right in personal information given voluntarily by an individual to private parties.(3)

In the landmark case of *Smith v. Maryland*, for example, the defendant claimed that information in the form of telephone numbers he dialed from his home telephone could not be turned over to the police absent a search warrant. Rejecting this argument, the Supreme Court noted that it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."

In *United States v. Miller*, a case involving a bootlegger's private financial records which were given by a bank to U.S. Treasury agents, the bootlegger's attempt to have this evidence excluded was unsuccessful. The Court found that Miller had no expectation of privacy in the bank records, reasoning that "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government..." The records could not therefore be considered confidential communications because they had been voluntarily conveyed by Miller to the bank in the "ordinary course of business."

Analogizing to the private sector's use of biometrics, the Court's reasoning in *Smith* and *Miller* suggests that the Court would be reluctant to find a reasonable expectation of privacy in biometric identification information provided in connection with a private sector activity. Rather, the Court would likely view the biometric identification information as having been voluntarily provided by the individual to another party in the ordinary course of business. Thus, the Court would find that, just like the depositor, the individual takes the risk, by providing his biometric identification information to another, that the information will be conveyed by that private party to others, including the government.

Despite the Court's likely reluctance to expand individual privacy protections related to private sector use of biometrics, Congress can have the ultimate word. Again, *Miller* is instructive. Following the *Miller* decision, Congress, in 1976, passed the Right to Financial Privacy Act (RFPA) (12 U.S.C. 3401 *et seq.*) to establish procedural requirements for financial institutions when disclosing information to the government. Thus, the refusal of the Supreme Court to find a Constitutionally-mandated privacy right does not as a practical matter end the debate. Congress is free to act by passing legislation to protect information privacy. Similarly, the states are also free to act by regulating.

For private sector intrusions into privacy, the common-law, through its doctrines of contract, tort and

property, has, in varying degrees, attempted to provide certain protections for the individual. However, the law has not used these doctrines to protect individual information in private sector databases. Generally, as a matter of law, an individual in possession of information has the right to disclose it.

Accordingly, the private sector enjoys great leeway as far as what it can do with an individual's information. As two privacy scholars have concluded: "Except in isolated categories of data, an individual has nothing to say about the use of information that he has given about himself or that has been collected about him. In particular, an organization can acquire information for one purpose and use it for another ... generally the private sector is not legislatively-constrained."(4)

B. Examination of the Policy Status Quo

At present, Congress and the state legislatures have left biometrics essentially unregulated from the standpoint of individual privacy protections related to private sector use. However, Congress and several state legislatures have mandated the use of biometric scanning for certain public sector applications.

At the federal level, for example, Congress specifically required that the Secretary of Transportation, through the Federal Highway Administration (FHWA), "...shall prescribe regulations on minimum uniform standards for a biometric identification system to ensure the identification of operators of commercial motor vehicles."(5) In mandating this biometric identification system, Congress responded to public safety concerns that commercial truck drivers were allegedly obtaining concurrent commercial licenses from various individual states in an attempt to minimize the true extent of their traffic violations.

In 1996, Congress required the use of a biometric identifier in connection with border crossing identification cards for aliens entering the U.S. The relevant language reads:

The term "border crossing identification card" means a document of identity ... issued to [qualifying aliens] ... Such regulations shall provide that (A) each such document include a biometric identifier (such as the fingerprint or handprint of the alien) that is machine readable and (B) an alien presenting a border crossing identification card is not permitted to cross over the border into the United States unless the biometric identifier contained on the card matches the appropriate biometric characteristic of the alien.(6)

Similarly, legislatures in several states have authorized the use of biometric identifiers as a condition of enrollment for certain entitlement programs, most notably welfare assistance. For example, states including Arizona, California, Connecticut, Illinois, Massachusetts, New Jersey, New York and Texas are using finger imaging to prevent entitlement fraud. Florida, North Carolina and Pennsylvania have biometric operational systems pending.(7)

What is important, however, is what Congress and the state legislatures have not done. Despite these forays into the world of biometric applications, Congress and the state legislatures have taken precious few steps to regulate biometrics related to privacy concerns stemming from private sector use. Among the states, California has moved in this direction. Recently, Assembly Member Kevin Murray, with the support of the California Banker's Association as well as the Center for Law in the Public Interest, introduced legislation (AB 50) to promote the responsible use of biometric identifiers to prevent identity theft while preserving the security of customer information. The bill's key provisions include:

A prohibition against selling, exchanging or otherwise providing

biometric identification databases to third parties;

A mandate that electronic storage of biometric identifiers be carried out in

the same manner as a company's confidential information;

A prohibition on recording someone's voice for biometric

identification purposes without their consent; and,

A prohibition against the discriminatory use of biometric

identifiers.

The federal government's executive branch has taken impressive initiatives with respect to biometric research and applications. For example, the Biometric Consortium (BC), chaired by Jeffrey Dunn, is the United States Government's focal point for research, development, testing, evaluation and application of biometric-based technology. However, to date, the executive branch has not attempted any wide-ranging regulation of biometric activities in the private sector. While the Department of Commerce and Federal Trade Commission, for example, have shown concern for various privacy issues, they have not yet delved deeply into the biometric arena.

III. Biometrics as Privacy's Friend

A. Biometrics Protects Privacy by Safeguarding Information Integrity

While critics of biometrics contend that this new technology is privacy's foe, the opposite is, in fact, true. Biometrics is a friend of privacy whether used in the private or public sectors. Biometrics proves itself as privacy's friend when it is deployed as a security safeguard to prevent identity theft and fraud.

To consider a specific example drawn from the financial services industry but applicable to almost any fraud prevention scenario, criminals eagerly exploit weaknesses with the present access systems, which tend to be based on passwords and PINs, by clandestinely obtaining these codes. They then surreptitiously access a legitimate customer's account. The honest client effectively loses control over her personal account information. Her financial integrity is compromised and her finances are gone because a criminal has gained unauthorized access to the information. In effect, she has suffered an invasion of her privacy related to her financial integrity. With biometric-based systems, identity theft, while never completely defeated, becomes more difficult for the criminal element to perpetrate. The use of biometrics means less identity theft and less consumer fraud which means greater protection of consumers' financial integrity.

Numerous examples exist of impostors masquerading under false identity which biometrics could

prevent. For example, James E. Young (Young 1) suffered financial losses as well as loss to his reputation when a person with the same first and last name (Young 2) was able to get Young 1's undergraduate transcript from his state university. This transcript contained extensive personal information including Young 1's social security number. Young 2 then used this information to establish charge accounts where he purchased items billable to Young 1.(8) In such a case, biometric applications would almost certainly help protect a citizen's informational integrity by making it more difficult for the criminal to get the information; Young 2's biometric would not match Young 1's.

B. Biometrics Used to Limit Access to Information

Biometrics becomes a staunch friend of privacy when the technology is used for access control purposes, thereby restricting unauthorized personnel from gaining access to sensitive personal information. For example, biometrics can be effectively used to limit access to a patient's medical information stored on a computer database. Instead of relying on easily compromised passwords and PINs, a biometric identifier is required at a computer workstation to determine database access. The same biometric systems can be used for almost any information database (including Internet databases) to restrict or compartment information based on the "Need to Know" principle.

Biometrics also protects information privacy to the extent that biometrics can be used, through the use of a biometric log-on explained above, to keep a precise record of who accesses what personal information within a computer network. For example, individual tax records would be much better protected if an Internal Revenue Service official had to use her biometric identifier to access them, knowing that an audit trail was kept detailing who accessed which records. Far less snooping by curious bureaucrats would result.

C. Biometrics as Privacy Enhancing Technology

In addition to safeguarding information integrity and limiting access to sensitive information, biometrics can also enhance privacy in broader ways. For example, biometrics can be used to control access to information, such as financial records, without requiring specific identification of the person accessing the information. In this way, privacy is enhanced by ensuring that only authorized persons can access the information, but obviating the need to specifically identify those individuals who have accessed the information. There are several biometric technologies which use the individual's physical characteristic to construct a digital code for the individual without storing the actual physical characteristic in a database.(9) For example, in one such system, using finger image-based technology, a person's fingerprint is digitized, encoded, encrypted and entered onto the access list. This encrypted access code can only be decoded by a match with the appropriate finger pattern, thereby reducing the fraud risk. At the same time, only the encrypted access code, and not the actual fingerprint, is stored in the database. In this regard, the anonymous verification system protects financial privacy.

The applications of this type of anonymous verification system are extensive. Most notably, such a biometric-based system would seem to provide a ready commercial encryption capability. Moreover, rather than technological advances eroding individual privacy expectations as has transpired, for example, with the Environmental Protection Agency's use of a special aerial surveillance camera to photograph private property,(10) biometrics, as used to create an anonymous encryption system, would provide for privacy enhancement.

While criticisms of biometrics deserve attention, particularly with respect to government-mandated use of the technology, many of the criticisms of biometrics are off the mark in that they should really be aimed at the exploitation of contemporary information systems which are the result of America's

economic, political and technological changes. Moreover, the criticisms fail to acknowledge that in many situations knowing an individual's identity is necessary and prudent.(11) As the next section explains, the use of biometrics might provide for even further individual privacy protections through a phenomenon known as biometric balkanization.

IV. Biometric Centralization vs. Biometric Balkanization: Which Protects Privacy Better?

It is important to address whether a specific biometric technology will come to dominate biometric scanning systems. In other words, will the biometric future feature biometric centralization whereby one biometric would dominate multiple applications, or will we see biometric balkanization (also known as biometric diversity) where multiple biometrics are used for multiple applications? At present, finger imaging has an early lead in terms of industry presence and received an important seal of governmental approval when it was endorsed by the General Accounting Office.(12) The popularity of finger imaging is explained primarily by its consistency and uniqueness, the fingerprint's long acceptance by the public, and extensive competition in the finger imaging market leading to rapidly decreasing user costs, among other factors.

For example, with regard to public acceptance of finger imaging, a survey of 1,000 adults revealed that 75 percent of those polled would be comfortable having a finger image of themselves made available to the government or the private sector for identification purposes. This high acceptance is arguably underscored by over half of those surveyed saying they had been fingerprinted at some point in their lives. Only twenty percent thought that fingerprinting stigmatizes a person as a criminal.(13)

Despite this early lead, however, it is not clear that finger imaging will emerge as the biometric of choice. It is tempting to predict that finger imaging will dominate the market because of its perceived advantages. This view, however, overlooks one of the great strengths of the current biometric market: It offers many robust technologies which allow maximum choice for users. A more likely outcome is that biometric balkanization will result: Multiple biometrics will be deployed not only by various public and private sector actors but multiple biometrics will be deployed by the same actor depending on the specific mission.

Arguably, biometric balkanization, like its Eastern European namesake, can take on a sinister spin. Individuals will be forced to give up various identifying "pieces" of themselves to countless governmental and corporate bureaucracies. In an Orwellian twist, the retina, the iris, the fingerprints, the voice, the signature, the hand, the vein, the tongue and presumably even the body odor could all be extracted by the State and stored in databases.

Yet, biometric balkanization offers at least two key advantages for the protection of privacy. First, biometric balkanization offers maximum flexibility to the private or public actor that will use the technology. The actor can tailor a specific biometric program to meet its own unique mission within its resource constraints. Depending on the situation and the degree of accuracy in identification required, the optimal biometric for that use can be selected. For example, the best biometric used to verify access to a government entitlement program might differ from the best biometric used by a university to ferret out undergraduate examination fraud, which in turn might differ from the best biometric needed in a

prison environment where hostile users will go to extreme lengths to foil identification efforts. Similarly, voice verification might be ideal for determining account access over the telephone while signature dynamics might be better suited for the tax authorities monitoring returns.

Secondly, biometric balkanization might actually mean a synergy of the actors' interest and the individual's concerns. Consider, for example, the public sector use of biometrics: Government agencies basically want dependable, workable biometrics to achieve their primary purpose -- verifying or identifying an individual. The individual essentially wants the same thing, plus protection of private information. If different technologies are used for different situations, citizens will not face the necessity of reporting to the government's "biometric central" for enrollment. By allowing the agencies maximum choice of biometric technologies, the individual gains greater protection for private information.

Biometric balkanization could also lead to the safeguard of biometric compartmentation which would be achieved through the use of different biometric identifiers. For example, an iris pattern used for automated teller machine (ATM) access would be of little use to a state's Department of Social Services which uses finger imaging just as a finger geometry pattern captured at Disney World would be of little value to tax authorities investigating phony signatures on fraudulent tax returns from the Sunshine State. From the privacy enhancement perspective, biometric balkanization is the equivalent of being issued multiple identification numbers or PINs or passwords with the important difference that biometric-based systems provide better security and greater convenience.

On balance, however, the greater threat to privacy with respect to biometric applications will likely not arise from the use of advanced technology to monitor but rather from sloppiness in database management. The potential for a breach in database security increases greatly as shortcuts are taken, budgets are slashed, trained personnel are few and leaders do not draft and implement plans to safeguard biometric identification information for which they are responsible. Accordingly, limited government regulation, based on the CFIP principles discussed below, should be viewed as biometric technology-promoting and not biometric technology-opposing.

V. How Should Privacy Concerns Be Safeguarded? The Need for a Biometric Blueprint

In balancing the privacy concerns with the benefits biometrics provides in private sector applications, several options exist for our nation's policymakers. To summarize, these options include:

1. *Laissez-faire* Approach, *i.e.* "If it ain't broke, don't fix it";

2. Self Regulatory Approach, based on voluntary industry codes;

3. Government Regulatory Approach, at the state or federal level; or

4. Hybrid Approach, featuring a combination of the above.

In my view, Congress should encourage biometric applications by mandating the adoption of a biometric blueprint based on a Code of Fair Information Practices (CFIP). The federal government should promote biometrics by requiring the private sector to adhere to a sensible CFIP-based biometric blueprint.

The adoption of a biometric blueprint at the federal level is an effective way to balance privacy concerns with the benefits of biometrics. We are well aware of problems of identity theft and consumer fraud resulting from the compromise of traditional forms of personal identification such as names, addresses, social security numbers and driver's license numbers. Moreover, just like an individual who gives personal information in other non-biometric contexts, the individual providing biometric identification information to an organization can similarly expect that his information will be used for the specific purpose for which he gave it and in his best interest, not in any way to his detriment. The individual does not expect to be annoyed, pressured, harassed or harmed by its use.

As a bedrock premise, a CFIP establishes rights for data subjects and places responsibilities on the data collectors. In this sense, it provides for the mutuality of control of the information provided. The CFIP-based Congressional biometric blueprint should consist of five basic principles which include:

1. *Notice*: The clandestine capture of biometric identification information in the private sector would be strictly prohibited. No secret databases should exist.

2. *Access*: The individual (or data subject) has the right to access his information in the database. Specifically, the individual must be able to find out if his biometric identification information is in the database and how it is being used by the data collector. Accordingly, the data collector would be required to disclose its privacy practices.

3. *Correction Mechanism*: The individual must be able to correct or make changes to any biometric identification information in the database. As one of the technical advantages of biometrics is that they are based on physical characteristics or personal traits which rarely change over time, this principle would likely not be called into play too often.

4. *Informed Consent*: Before any information can be disclosed to third parties, the individual must consent. The individual must voluntarily and knowingly provide his biometric identification information to the data collector in the primary market. Once in the possession of the data collector, this information would then be governed by a use limitation principle. This means that the individual has consented that the information she provided would be used in the primary market for a purpose defined by the data collector and known to the individual. The individual must knowingly consent to any exchange, such as buying and selling of his biometric identification information, before it could be traded in a secondary market. Reasonable exceptions can be accommodated as appropriate for academic research and law enforcement, for example.

5. *Reliability & Safeguarding*: The organization responsible for the database must guarantee the reliability of the data and safeguard the information. Any data collector that collects and stores biometric identification information must guarantee the reliability of the data for its intended use and must take precautions to safeguard the data. At its most basic level, appropriate managerial and technical controls must be used to protect the confidentiality and integrity of the information. The controls would include making the database and the computer system physically secure. Data collectors should explore the option of encrypting the biometric data to help further safeguard the information from disclosure. Perhaps, policymakers should consider providing criminal sanctions for willful disclosures, or consider providing for the recovery of civil damages when biometric identification information is disclosed

without the consent of the individual.[14]

Policymakers could also explore various options to ensure compliance with the biometric blueprint. For example, Congress could assign this task directly to a federal agency. Alternatively, Congress could consider establishing a self regulatory organization to handle these duties. Congress could also decide whether it should require an assurance program designed to help guarantee compliance with the biometric blueprint. For example, a prime goal of such an assurance program would be to make certain there had been no dissemination of biometric identification information to unauthorized third parties.

VI. Conclusion

In attempting to answer whether new privacy protections are necessary in the face of the new technological reality of biometrics, I urge policymakers in the executive and legislative branches to take a forward-looking approach to how the law can sensibly regulate this new, dynamic technology. Privacy concerns related to biometrics can best be accommodated by legislative enactment of a limited yet uniform biometric blueprint to provide a framework to address legal and policy issues related to the private sector's use of biometrics. This biometric blueprint would cover private sector users of biometrics. In doing so, the blueprint would comfortably mesh with existing CFIP principles.

We are now eyeball to eyeball with a new, exciting technology that can be used in robust ways by the public and private sectors. A biometric blueprint can be used to make this new technology even more acceptable and beneficial for private sector use, particularly with regard to Internet applications. It is surely better to have a far-sighted biometric policy that deals with the face of a new technological reality now than to point fingers of blame later.

Appendix I

Biographical Information

John D. Woodward, Jr.

John D. Woodward, Jr., an attorney, lectures and writes regularly on the law and policy concerns of biometrics. He has testified before Congress on this topic and has authored numerous articles on biometrics which have been published in *University of Pittsburgh Law Review*, *Proceedings of the IEEE*, *American Banker*, *Biometric Technology Today*, *Information Security*, *Legal Times*, *CTST '98 Proceedings*, *CTST '97 Proceedings*, and *CTST '96 (Government) Proceedings*.

Mr. Woodward has written articles on other legal and professional topics which have appeared in *Asian Manager, Far Eastern Economic Review, Inside Japan Journal, International Quarterly for Asian Studies, Money Laundering Law Report* and others. Before practicing law, he served as an Operations Officer for the Central Intelligence Agency for twelve years. In his last assignment, he was the CIA Staff Assistant to the Under Secretary of Defense for Policy at the Pentagon. Mr. Woodward's overseas assignments included tours in East Asia and Africa. He speaks Japanese and Thai.

Mr. Woodward, a member of the Virginia State Bar, received his Juris Doctor degree *magna cum laude* from Georgetown University Law Center in Washington, D.C. He was a Thouron Scholar at the London School of Economics, University of London, where he received his M.S. in Economics. He received his B.S. in Economics from The Wharton School of the University of Pennsylvania. He resides with his wife, Shirley Cassin Woodward, in Madison County, Virginia.

1. These comments are based on my testimony before a hearing on "Biometrics and the Future of Money" before the Subcommittee on Domestic and International Monetary Policy of the Committee on Banking and Financial Services of the U.S. House of Representatives, chaired by the Hon. Michael N. Castle, on May 20, 1998. I gratefully acknowledge the assistance of Arthur S. DiDio, M.D., J.D., and Professor Steven Goldberg of Georgetown University Law Center who kindly reviewed my testimony and contributed comments. Biographical information about the author is included at Appendix I.

2. Charles Fried, AN ANATOMY OF VALUES, 140 (1970); Richard B. Parker, *A Definition of Privacy*, 27 RUT. L. REV. 275, 281 (1974);Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 236 (1977); United States v. Westinghouse Elec. Corp., 638 F. 2d 570, 577 (3rd Cir. 1980)(holding that medical records of a private sector employee, while within the ambit of constitutional privacy protection, could nonetheless be disclosed to a government agency upon a proper showing of governmental interest). *See also* Fred H. Cate, Privacy in the Information Age 19-31 (1997).

3. *See* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

4. MARC ROTENBERG & EMILIO CIVIDANES, THE LAW OF INFORMATION PRIVACY: CASES & COMMENTARY 22 (1997).

5. The Truck and Bus Safety and Regulatory Reform Act of 1988, Pub. L. No. 100-690, Section 9105(a), 102 Stat. 4530 (1988), (codified as amended at 49 U.S.C. Section 31309(d)(2) (1994)).

6. The Immigration and Nationality Act (as amended). *See also* 8 U.S.C.A. Section 1101(a)(6) (West Supp. 1997).

7. *See* Brian J. Wing, *New York State Department of Social Services: Automated Finger Imaging*, (March 1997) at 677-684, in CTST '97 CONFERENCE PROCEEDINGS (1997)(explaining how "New York State has implemented the nation's first statewide automated finger imaging system (AFIS) for the identification of public assistance recipients."); David Mintie, *Biometrics for State Identification Systems -- Operational Experiences*, in CTST '98 CONFERENCE PROCEEDINGS (1998).

8. *See* State ex rel. Beacon Journal Publishing Co. v. Akron, 70 Ohio Sr. 3d 605 (1994).

9. *See, e.g.,* Ann Cavoukian, *Privacy and Biometrics: An Oxymoron or Time to take a Second Look?* presented at Computers, Freedom and Privacy '98 (1998).

10. *See* Dow Chemical Co. v. United States, 476 U.S. 227 (1985)(holding that Dow had no reasonable, legitimate and objective expectation of privacy in the area photographed); *see also* United States v. Knotts, 460 U.S. 276 (1983).

11. For a discussion of the criticisms of biometrics, *see, e.g.,* John D. Woodward, *Biometrics: Privacy's Foe or Privacy's*

Friend?, 85 Proceedings of the IEEE 1480 (1997). For a discussion of the concerns raised by government-mandated use of biometrics, *see, e.g.*, John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns; Drafting the Biometric Blueprint*, 59 U. Pitt. L. Rev. 97 (1997).

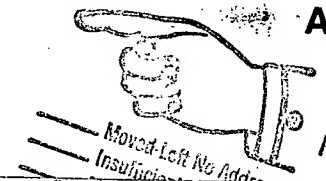
12. United States General Accounting Office, Electronic Benefits Transfer: Use of Biometrics to Deter Fraud in the Nationwide EBT Program, GAO/OSI-95-20, Sept. 1995 (prepared at the request of Representative Kenneth E. Bentsen, Jr.).

13. *See* "People Patterns: Fingerprints? No Problem," *Wall Street Journal*, Jan. 31, 1997.

14. *See, e.g.*, Whalen v. Roe, 429 U.S. 589, 593-595 (1977)(but note that in *Whalen*, these criminal sanctions applied to unauthorized disclosure from a government-mandated database containing the names and addresses of patients receiving certain prescription drugs).

Organization TC2100 Bldg./Rm. RANDOLPH
U. S. DEPARTMENT OF COMMERCE
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
IF UNDELIVERABLE RETURN IN TEN DAYS

OFFICIAL BUSINESS



Moved-Left No Address
Insufficient Address
Forwarding Order Expired
Attempted Not Known
Route Number
Vacant
Unclaimed

AN EQUAL OPPORTUNITY EMPLOYER

UNITED STATES POSTAGE
02 1A
0004204479
MAILED FROM

RECEIVED
APR 21 2006
USPTO MAIL CENTER